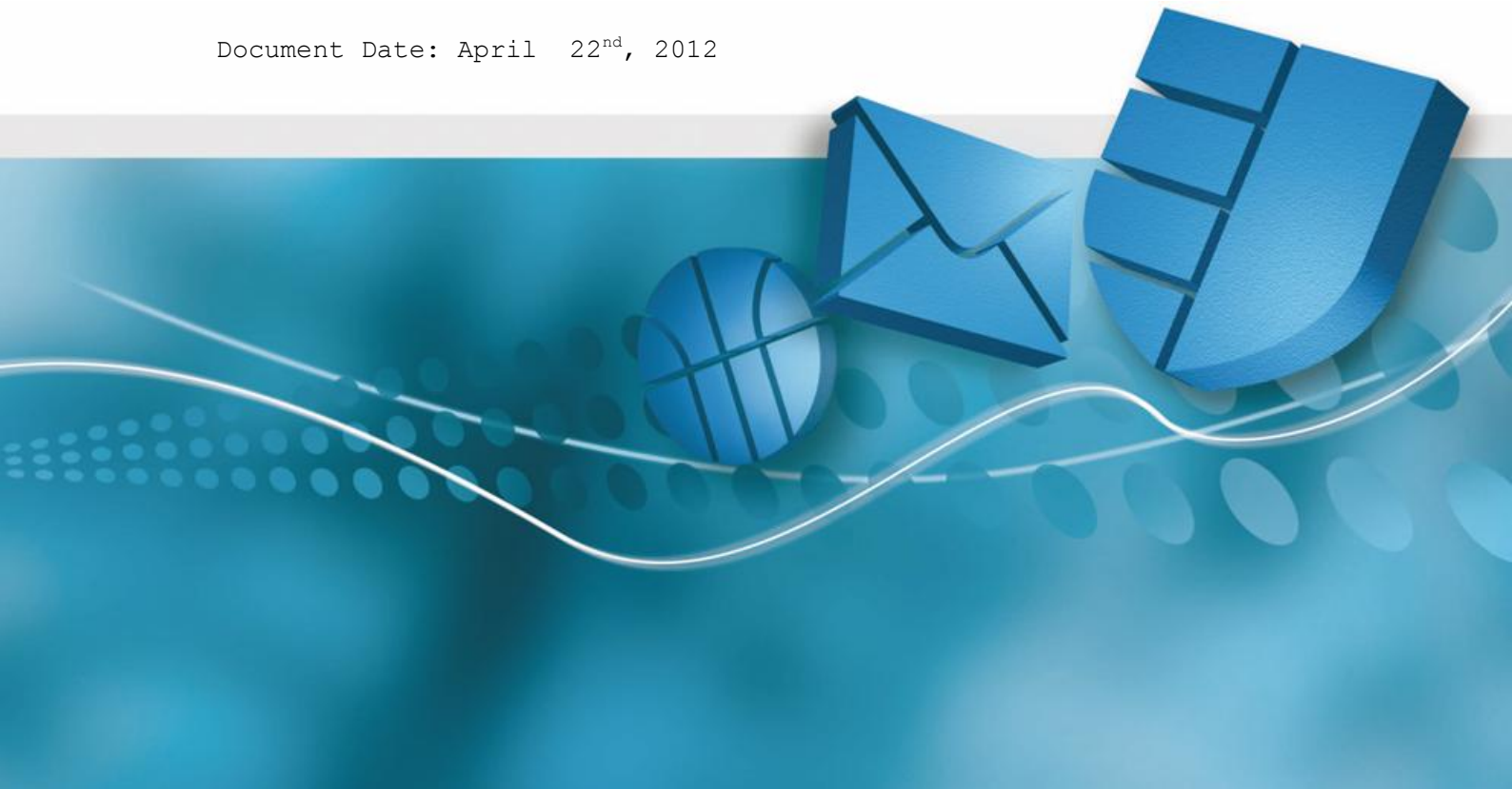
SOPHOS

SafeGuard Enterprise 6.0

Technical white paper

Document Version: 6.0

Document Date: April 22nd, 2012



Contents

1 Introduction 3

2 SafeGuard Enterprise functions 4

2.1 Overview 4

2.2 SafeGuard Management Center 5

2.3 SafeGuard Device Encryption 6

2.4 SafeGuard Data Exchange 8

2.5 SafeGuard Encryption for File Shares 9

2.6 SafeGuard Encryption for Cloud Storage 9

2.7 SafeGuard Configuration Protection 9

2.8 Security Engine 9

3 SafeGuard Enterprise architecture 11

4 SafeGuard Management Center 12

4.1 Overview 12

4.2 Flexible policy creation and assignment 12

4.3 Additional selected administration functions 15

5 SafeGuard Enterprise encryption methods 22

5.1 Overview 22

5.2 Smart Media Encryption 22

5.3 Power On Authentication 25

5.4 Smartcard and token integration 27

5.5 Emergency scenarios 27

5.6 SafeGuard Enterprise BitLocker client 27

6 Appendix 30

6.1 Technical data 30

6.2 Migration from existing SafeGuard products 31

6.3 New in SafeGuard Enterprise 6 31

7 Abbreviations 32

8 Literature and Sources 34

1 Introduction

Stored information is one of a company's most important assets. As more confidential and valuable data is carried around by employees, protecting sensitive enterprise data—especially in mobile computing—is more important than ever. The tried-and-trusted protection provided by a company's central firewall is useless for mobile clients. Mobile clients or removable media are particularly vulnerable to loss or theft, which makes them a weak spot in a modern IT infrastructure. Companies need a security solution that not only can protect them against this threat, but also ensure that unauthorized persons cannot access their stored data and the rest of their IT infrastructure.

This white paper introduces SafeGuard Enterprise, an innovative product from Sophos that fulfills all the requirements a company could have for protecting mobile PCs and data media. With many years of experience in the information security business, Sophos is well versed in the security challenges faced by companies of all sizes in many different countries and different business sectors, and utilizes this expertise in its product developments.

This document begins with an introductory overview of existing and planned SafeGuard Enterprise modules, followed by a detailed description of the most important aspects of the product:

- Efficient implementation of company-wide security guidelines
- Informative software inventory reports and reports that are relevant to security events
- Effective protection for mobile PCs, ports and data media
- Great ease of use, with highly versatile key management
- Powerful, flexible user authentication
- Future-proof, extendable system architecture

To aid understanding, the last section describes the most frequently used abbreviations.

This is a technical white paper that focuses on Sophos's SafeGuard Enterprise product. Please refer to the separate white paper [Mobile security] for introductory and more detailed information about the general (business) benefits of SafeGuard Enterprise.

2 SafeGuard Enterprise functions

2.1 Overview

SafeGuard Enterprise (SGN) protects data against data theft and ensures that it remains confidential, no matter where it is stored.

Its underlying architecture was developed with the aim of enabling seamless integration in the existing IT environment, while ensuring that neither the security administrator nor the users of the security solution are restricted in their daily work. With the central administration and reporting functions, the administrator can implement the security guidelines on all devices at any time from one central point, and then use the SafeGuard Management Center to check the implementation. At the same time, end users are not restricted in their work by the additional security provided by SGN and need no special training.

SafeGuard Enterprise's combination of transparent data medium and file encryption (Smart Media Encryption), together with its keyring concept, achieves levels of flexibility in protecting data media and the information saved on them that until now could not be obtained in the market.

The portfolio of authentication methods for users is constantly being extended, permitting the integration and use of existing smartcard and PKI structures, and providing an easy way to change over to them if they are required in a company in the future.

SafeGuard Enterprise is the result of many years of IT security experience. The product was developed in accordance with current standards and has a modular structure. These factors ensure it has the highest level of interoperability and flexibility for any future upgrades.

All of SafeGuard Enterprise's functions are designed for use in professional business environments and can be managed from a central point. SafeGuard Enterprise does not require any new user accounts or devices to be set up. It uses the information present in Active Directory instead. The Management Center is also structured in such a way that it can be used for multi-platform tasks, so that in the future both PCs and PDAs/smartphones can be managed at the same time.

Figure 1 shows the main modules of SafeGuard Enterprise in their future final stages of development:

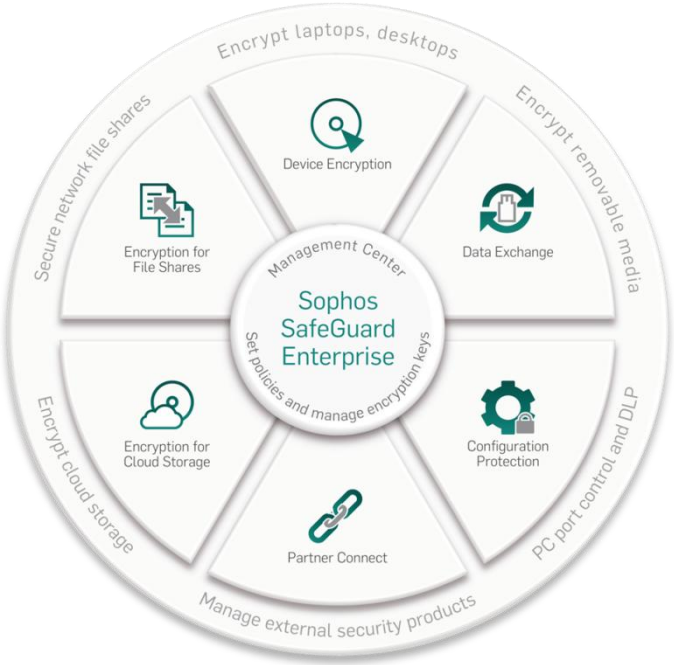


Figure 1: SafeGuard Enterprise overview

2.2 SafeGuard Management Center

The Management Center is the central controlling module in SafeGuard Enterprise. Its primary tasks include:

- The centralized creation and administration of security guidelines (security policies) in modular, inheritable units
  → *SafeGuard Enterprise enables the efficient creation of policies even in large-scale environments.*
- The distribution of policies to all SafeGuard Enterprise clients via direct, secure web service communication (Simple Object Access Protocol [SOAP])
  → *SafeGuard Enterprise ensures that central policies are implemented quickly on the clients.*
- The re-use of existing infrastructure data by optionally importing it from Active Directory
  → *SafeGuard Enterprise does not require any additional new user or machine administration; rather, existing information is used. Instead of using Active Directory import, auto registration may be used as an alternative that does not require any directory system to be in place. Furthermore, the SGN Management API provides a second alternative for machine/user import and allows*

the linking of SGN to any provisioning or directory system (e.g., Novell eDirectory) via customized scripts.

- Centralized logging and reporting of status and licensing information
  → *SafeGuard Enterprise provides information about network procedures that impact security issues and facilitates the provision of proof to government bodies that end devices have been encrypted (e.g., regulatory compliance in the United States).*
- The administration of certificates and smartcards
  → *SafeGuard Enterprise uses existing PKI infrastructures if they are present, but this is not a requirement.*
- Providing the option of role-based administration, such as Security Officer and Audit Officer
  → *This is a simple method of achieving a "division of power" between the network administrator and the security administrator for encryption or other administrative roles.*
- Monitoring the "health status" of SafeGuard Enterprise Management Servers via the optional Management Pack for Microsoft System Center Operations Manager (SCOM) 2007
  → *In large IT infrastructures that are monitored with SCOM 2007, this monitoring can be extended to SafeGuard Enterprise. For details, see the separate white paper [SGN SCOM].*

2.3 SafeGuard Device Encryption

The Device Encryption module and the Management Center[1] are the main modules available in SafeGuard Enterprise. The task of the Device Encryption module is to protect end devices (PCs, notebooks, and netbooks) Although data on removable media can be protected as well, it is recommended to use the SafeGuard DataExchange module since it offers more flexibilty.

Since version 5.50, SafeGuard Device Encryption is available in "standalone mode" (without the Management Center), offered under the name SafeGuard Easy. This is the successor to the previous SafeGuard Easy product for customers who prefer the "install and

[1] Starting with version 5.30, the Device Encryption module optionally can be operated without SGN Management Center in standalone mode. For more details, see the Sophos white paper, "SafeGuard Enterprise/Easy Standalone Mode." Starting with version 5.50, this mode is available under the name SafeGuard Easy 5.50.

forget" management style of SafeGuard Easy as opposed to SafeGuard Enterprise's online management.

SafeGuard Device Encryption's primary tasks include providing:

- Transparent, sector-based encryption (volume-based encryption) of any data saved on local or external data media
  → *It protects the data if the device or data medium is lost or stolen. Because it runs transparently, users can simply continue working with their usual applications such as Microsoft Office. SafeGuard Enterprise ensures that* all *the data is encrypted (including boot files, swapfiles, hibernation files, temporary files, etc.) without requiring users to adapt their working habits or even to worry about security.*

- A flexible keyring concept
  → *This allows encrypted removable data media to be exchanged quickly and easily within specific user groups. It also facilitates recovery procedures in an emergency (e.g., a hard disk that will no longer boot can be inserted in a different computer on which the appropriate key is present).*

- The latest graphical 32-bit pre-boot authentication (Power On Authentication [POA]) before the actual operating system starts up; biometric fingerprint authentication with single sign-on to Windows is also supported at pre-boot time
  → *This reliably prevents the operating system from being manipulated from outside and also protects against the use of password hacking tools. SafeGuard Enterprise Power On Authentication provides an adaptable graphical user interface with full Unicode support for Asian languages and support for an extensive range of authentication hardware (smartcards, tokens, fingerprints). SafeGuard Enterprise also uses Windows accounts and passwords in its Power On Authentication. This removes the need for separate user management for Power On Authentication, which many competitor products still require.*

- Integration of Windows Vista/7 BitLocker Drive Encryption (BDE)
  → *This provides central management of BitLocker clients within the SGN Management Center, together with native SGN clients. It extends BitLocker using file-based transparent encryption for removable media. The SafeGuard Enterprise BitLocker module is available standalone (without SafeGuard Device Encryption) as well as via the Partner Connect module.*

- Management of self encrypted hard drives
  → Support and management of self encrypted hard drives which are following the Opal standard. The SG DE setup checks the hardware on the client and uses either the self encrypting drives technology or the SafeGuard encryption.

2.4 SafeGuard Data Exchange

The SafeGuard Data Exchange (SG DX) module transparently encrypts all kinds of removable media, and allows access to these media via password even on computers where no SafeGuard software is installed. All its functions and keys are centrally managed by the SafeGuard Enterprise Management Center[2].

When the SafeGuard Data Exchange (SG DX) module is used in combination with SafeGuard Device Encryption (SG DE), it adds important functions to the removable media encryption capabilities:

- Transparent file-based encryption on removable media
  → This ensures that all data stored on removable devices, including optical media such as CDs/DVDs, is encrypted and that data can be exchanged with external computers on which SafeGuard is not installed.
- Encrypted media can be used outside the organization. Users optionally can define their own keys or passwords for removable media, or the files stored on those media, and then exchange these keys or passwords with their business partners. These keys are then also stored on the central SafeGuard server for backup purposes, or can be assigned to other users by the administrator for recovery or sharing purposes.
- By policy, a mix of plaintext and encrypted files on the same media may be allowed, which is not possible for sector-based encryption.
- Optical media such as CD/DVD and Blu-ray may be encrypted with the DX module.
- The "Portable" component of the SafeGuard Data Exchange module also can be stored on the data medium. This allows encrypted removable media to be used on computers on which SafeGuard Enterprise is not installed. The keys generated with SafeGuard Portable also can be imported into a user's keyring so they can be used in SafeGuard Enterprise. Consistent, strong password rules and failed logon delays are also implemented for the portable functionality.

SafeGuard Data Exchange as a standalone solution is particularly suitable for customers who use SafeGuard Easy.

[2] Starting with version 5.30, the Data Exchange module optionally can also be operated without SGN Management Center in standalone mode. For more details, see the Sophos white paper, "SafeGuard Enterprise Standalone Mode."

2.5 SafeGuard Encryption for File Shares

The SafeGuard Encryption for File Shares (SG FS) module adds transparent file-based encryption. Designed primarily for protection of network file shares, it can also encrypt folders on local drives. (Even removable media folders, but in case of a policy overlap Data Exchange encryption rules have priority.)

By separating Security Officer roles for File Share administration from system administration, SafeGuard Encryption for Files Shares allows you to have an effective separation of duties. File Share Security Officers can be locked out from file system by using file system access control lists. System administrators can be locked out from the keys and policy management, too.

2.6 SafeGuard Encryption for Cloud Storage

Encrypt folders which are synchronized with the Cloud with this module. The file-based filter driver takes care that documents stored in the Cloud folders (e.g. Dropbox folder) are encrypted with keys provided by the SGN key ring. Central management is optional like in SG DX.

2.7 SafeGuard Configuration Protection

SafeGuard Configuration Protection (SG CP) prevents the PC from receiving potentially malicious code or unwanted exporting of confidential data via certain communication ports or peripheral devices. All its functions are centrally managed by the SafeGuard Management Center.

Besides read/write restrictions on ports such as USB, FireWire, WLAN and Bluetooth, just to name a few, the administrator also can configure policies based on device types, file types or even individual peripheral devices. For the latter, an easy-to-use tool is provided (the SafeGuard Auditor) that scans the clients on the network and centrally reports all actually or formerly connected peripheral devices as whitelist input for the policy.

2.8 Security Engine

The new Security Engine, which forms part of SafeGuard Enterprise, is the basis for every cryptographic operation. It has been developed to meet all current standards and with the specific aim of

achieving optimum flexibility and security. The Security Engine ensures that:

- Powerful encryption algorithms are present on all the supported platforms, including device drivers
- All the standards, algorithms and protocols relevant for this purpose are made available centrally
- Security certificates (e.g., FIPS, EAL) are applicable across these components
- New algorithms (e.g., customer-specific or country-specific algorithms) and crypto hardware (e.g., smartcards or tokens, Trusted Platform Modules) can be connected to SafeGuard Enterprise easily and effectively

3 SafeGuard Enterprise architecture

The inspiration behind SafeGuard Enterprise was the idea of combining many years of experience with the existing SafeGuard product portfolio, and to implement a modern, modular architecture to accompany users into the Windows Vista era and beyond. To achieve this aim, aspects were taken from established SafeGuard products and added to the requirements set out in current standards and concepts. However, a deliberate decision was made to eliminate full backward compatibility so that new concepts could operate to their best effect.

The design strategy behind SafeGuard Enterprise included, among other things:

- The incorporation of the very latest standards and protocols
- Scalable architecture for both the range of functions and the number of clients
- Comprehensive Unicode support for international implementation, especially in Asia
- A hierarchical administration concept with inheritable, modular policies
- A non-platform-specific nature to enable the subsequent integration of PDA and smartphone clients
- Extensive logging, auditing and inventory functions
- Secure policy storage and transfer
- Openness to the use of existing infrastructures (e.g., PKI, Active Directory, smartcards)

4 SafeGuard Management Center

4.1 Overview

The SafeGuard Management Center is the central point at which policies are created and then distributed to the users and clients that are being administered. Its user interface has been developed using the very latest .NET architecture. One or more Management Center consoles can be used within a company. SafeGuard Enterprise uses Active Directory as the source for infrastructure data, an SQL server for storing its own data and a web service for distributing policies to clients. All the communication is encrypted. Figure 2 shows the components and the data being transferred in a typical SafeGuard Enterprise scenario.

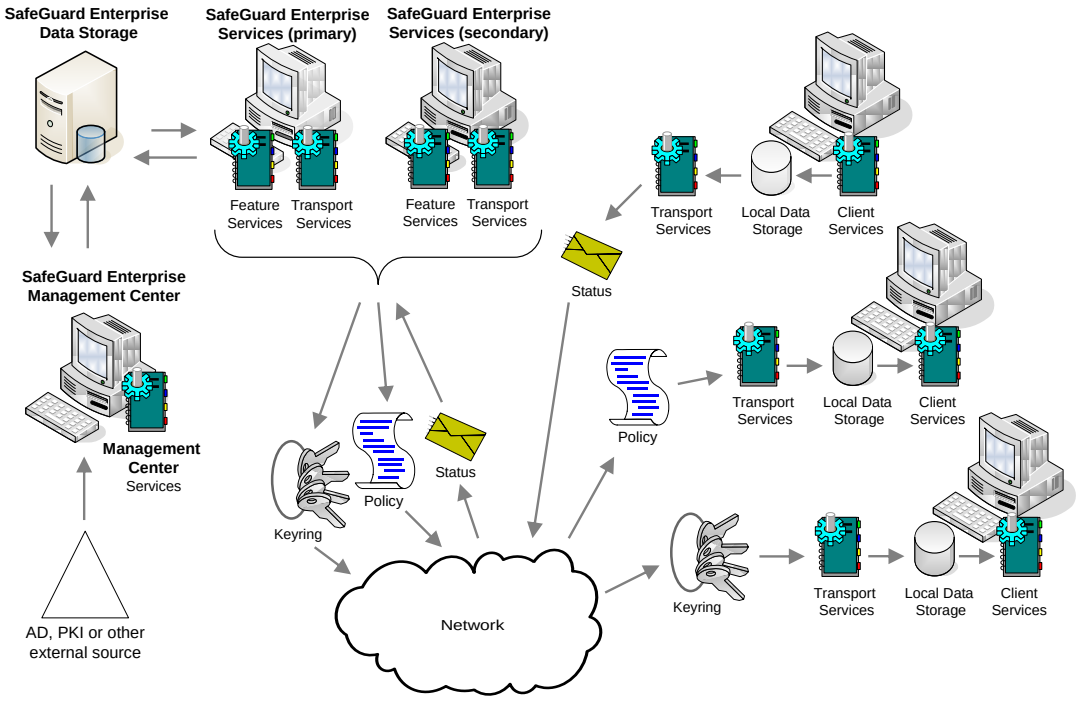


Figure 2: SafeGuard Enterprise administration components

4.2 Flexible policy creation and assignment

Once the infrastructure data has been imported from Active Directory, SafeGuard Enterprise can be used to create individual policy modules about specific topics, which can then be assigned to any existing organizational units. SafeGuard Enterprise can also inherit policies in the same way as in Active Directory. Therefore, administrators can, for example, create a general policy to govern

user logins for the entire domain and then assign different policies for data medium encryption to individual organizational units, or modify the login settings again for a specific group such as the directors. Security officers only ever need to define the information actually required by a specific group. Different policies that are often used together can, in turn, be combined to form template groups so that they can be assigned even more efficiently.

This enables SafeGuard Enterprise to achieve the flexibility required in today's distributed company environment. Therefore, it stands out from comparable products that often only allow one overall policy, without inheritance, to be used for each user group or even require product-specific user management procedures.

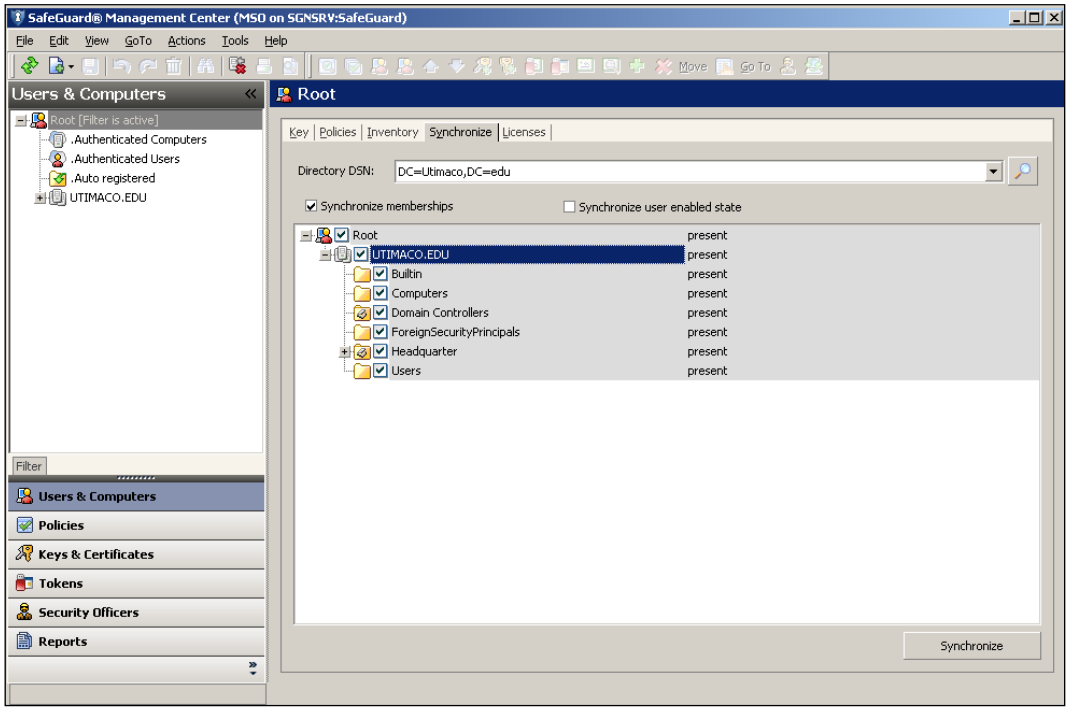


Figure 3: SafeGuard Enterprise Active Directory synchronization

SafeGuard Enterprise synchronizes its data with Active Directory without actually storing data in it or requiring write access to it (see Figure 3). This satisfies many administrators who are not happy to see different third-party applications making changes or creating schema extensions in Active Directory. SafeGuard Enterprise uses the advantages of Active Directory without having to modify it. Alternatively, SafeGuard Enterprise offers the auto-registration mode, in which SafeGuard Enterprise clients register themselves after installation in the Management Center. Furthermore, the SGN API may be used to provision the database via a customer-specific script connected to any third-party provisioning or directory system.

Both alternatives are ideal for customers who are not using Active Directory or who use a different directory system.

Figure 4 shows how an encryption policy is defined for all local disk drives, as an example. If necessary and if required by the administrator, this can be extended at a later time by the addition of a policy for specific data media (e.g., the boot partition or CD/DVD media). Each policy does not have to include all the settings. Values that are set to "not configured" are inherited automatically from other policies or filled with appropriate defaults, which can be displayed on the console at any time. With the RSOP function, effectively inherited policies can be displayed for a particular client or user. These functions run in the same way as those in Active Directory and therefore do not require any extra training for administrators.

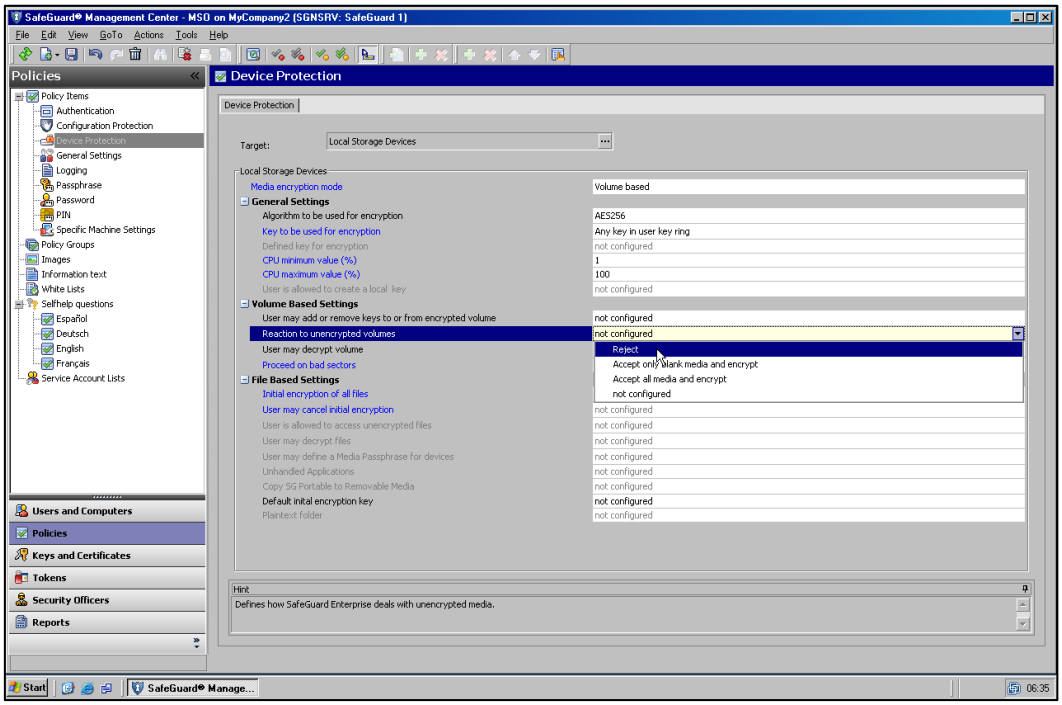


Figure 4: Defining a policy for all local data media

After one or more policies have been created, they are assigned to a manageable object (a group of users or machines) simply by dragging and dropping them (see Figure 5).

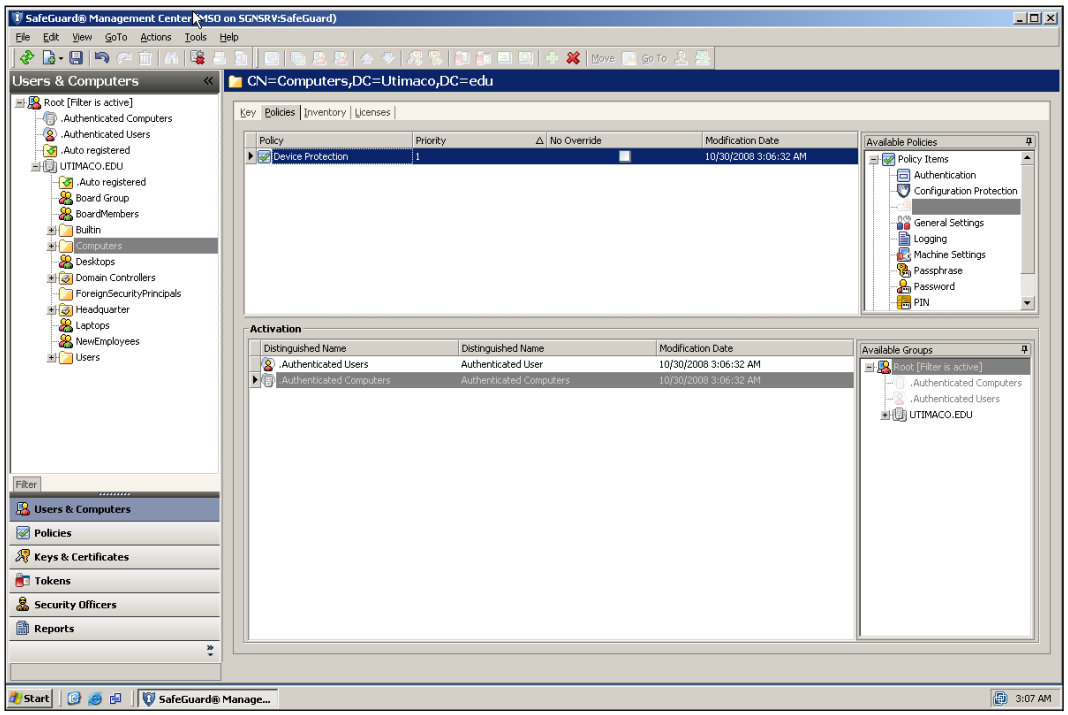


Figure 5: Assigning the "Default" policy to all computers

4.3 Additional selected administration functions

To describe every option in SafeGuard Management Center would go far beyond the scope of this white paper. However, we discuss a small selection of them in this section.

4.3.1 Flexible, modern key management

SafeGuard Enterprise's key management functions are entirely based on public key cryptography (certificates). Any Public Key Infrastructure (PKI) that is already present in a company can be used. If no PKI is present, SafeGuard Enterprise generates the keys it needs itself, in the form of self-signed certificates.

In SafeGuard Enterprise, every manageable object (users, groups and machines) has a key assigned to it. This is stored in an electronic keyring along with any inherited or specifically assigned keys. After logon has been completed, a user or machine has completely transparent access to all data for which the user or the machine has the appropriate key in the keyring. Consequently, a wide range of different scenarios, such as the following, can be implemented with ease:

- All removable data media are encrypted but can be freely exchanged within the company.

- Certain data media can only be exchanged within a particular user group.
- The user is given a private (personal) encrypted data medium.
- Central recovery and escrow functions are provided in case a user forgets his or her password or the user is no longer present.

4.3.2 Web service (SOAP)-based policy distribution

Policies are distributed asynchronously via a web service (SOAP). The benefit of this is that the SafeGuard Enterprise Management Server has a bidirectional link to the administered clients, so it can not only send policies to clients but also receive status information back. The client fetches policies from the server when it boots or at a configurable time interval, and buffers the most recently received policy locally. Due to this asynchronous working method, the user can remain productive even if there is temporarily no link to the server (e.g., if the client is offline). Optionally, clients can be blocked automatically if the time period during which they have not established a link to their server is too long. They must then be unblocked again, with the agreement of the help desk, via challenge/response.

SOAP also permits the use of the load distribution mechanisms provided in Microsoft's Internet Information Services, which means it is also scalable to suit the needs of large environments. It runs over standard ports, so there is usually no need to modify the firewall settings for SafeGuard Enterprise.

This distribution method is superior to traditional procedures such as, for example, providing policies in the form of file shares, in every way.

4.3.3 Central logging and status information

The bidirectional link to the client enables SafeGuard Enterprise to read a plethora of status and inventory data from clients and store or display it centrally. This not only provides the administrator with useful information, but also can provide proof that particular clients were encrypted at the time they were stolen. This proof is often required for legal reasons (e.g., in the United States). As would be expected, powerful sorting and filter functions are integrated in SafeGuard Enterprise, enabling administrators to find what they need in the plethora of information available. In addition, automated processing of the SafeGuard Enterprise log events (e.g., via Crystal Reports or Microsoft System Center Operations Manager) is supported.

For client encryption status reporting to external, non-SafeGuard, consoles, an SGNState utility is available to provide comprehensive information on the encryption status of a SafeGuard Enterprise client. Scripts can be used to trigger actions depending on the encryption status (e.g., when initial encryption is done), or simply for reporting SGN status information to a third-party management console such as LANDesk or Network Access Control (NAC) products.

All SafeGuard Enterprise log events are protected against unauthorized modification on both the client and server side by digital signatures, see Figure 6 below.

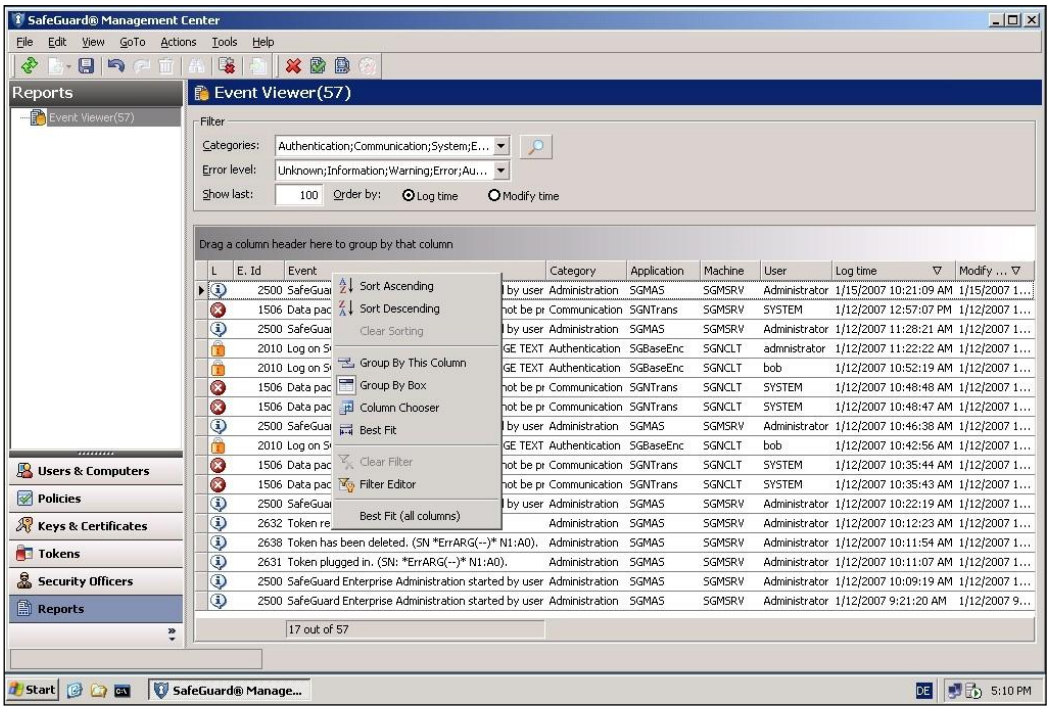


Figure 6: SafeGuard Enterprise Event Viewer

In addition to monitoring the encryption status of clients, the health status of the SafeGuard Management Center components (i.e., server, IIS, database) also can be monitored. A Management Pack is available for SafeGuard Enterprise that allows monitoring of the health status of the SafeGuard components within SCOM 2007 (see Figure 7). For more details, see the Sophos white paper [SGN SCOM].

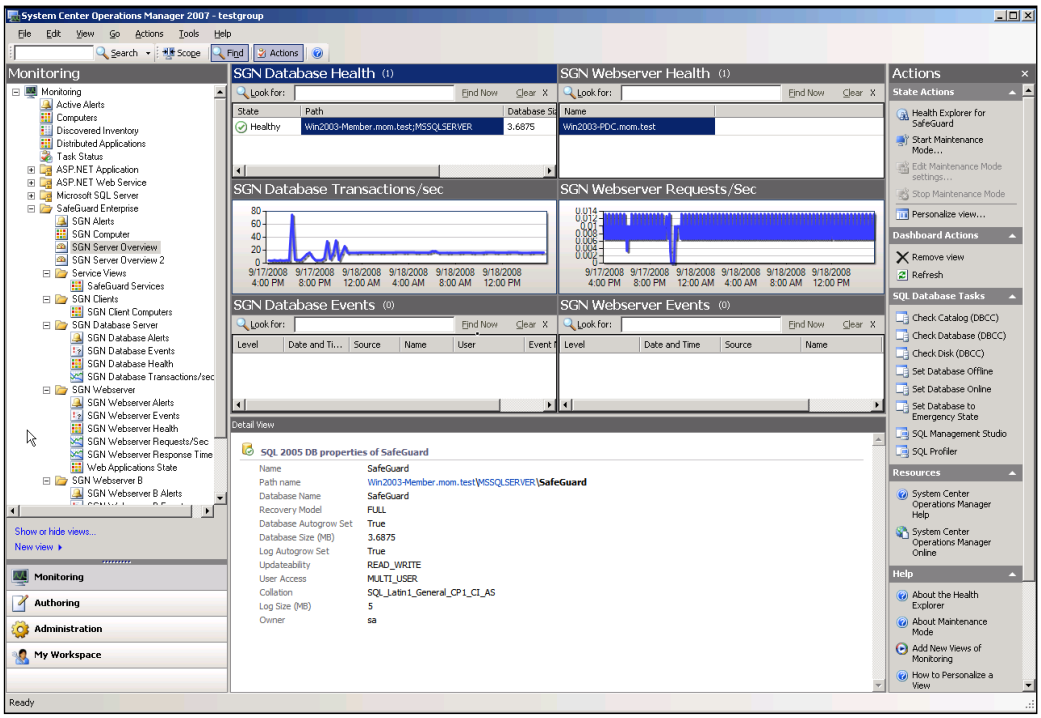


Figure 7: SGN Management Pack for SCOM 2007

4.3.4 Role-based administration

SafeGuard Enterprise offers flexibly configurable administrative roles, enabling the implementation of a form of separation of powers or simply assigning different authorizations to administrators (see Figure 8). Rarely performed administrative tasks that involve security can, if necessary, also require confirmation by a second administrator (i.e., two-person-rule or secondary authentication principle).

Administrative accounts also can be directly assigned to Active Directory users, which means no separate password management is required for them and enables the ability to lock or deactivate such an account directly via Active Directory.

Starting with SafeGuard Enterprise version 5.50, administrative rights can be inherited or delegated within hierarchies of administrators for easy and effective administrator management.

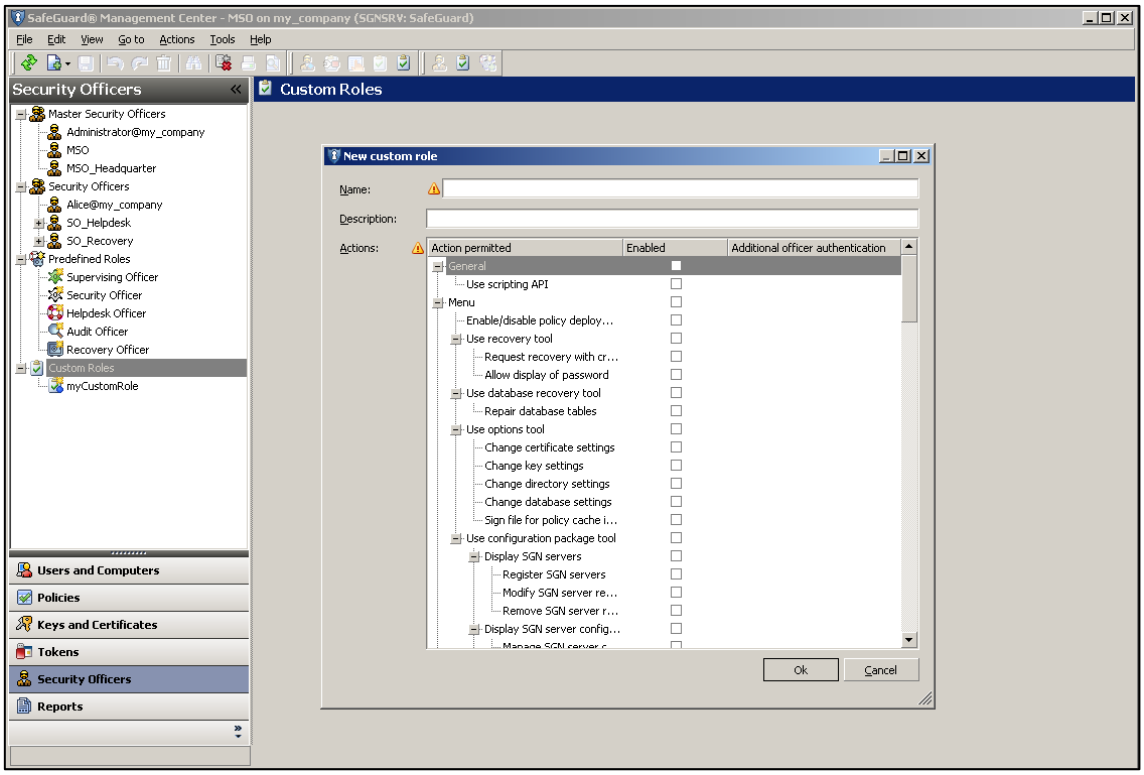


Figure 8: Definition of administrative roles

4.3.5 Web Helpdesk/Local Selfhelp

SafeGuard Enterprise offers various ways to make recovery and help desk tasks as efficient and flexible as possible. Besides providing administrative roles for help desk employees in the Management Center, customers may optionally choose to use the Web Helpdesk instead (see Figure 9). This enables help desk employees to perform their tasks via a customizable web interface, authenticating via any company-supported web authentication mechanism without requiring access to the SafeGuard Management Center.

Alternatively, the Local Selfhelp solution completely frees the help desk from the task of performing password resets, which reduces costs. Via this solution, any user can self-reset his or her password after correctly answering a series of pre-defined questions. Local Selfhelp is centrally configurable (see Figure 10) and supports custom question sets in multiple languages.

Local Selfhelp allows users to recover forgotten passwords even when they are offline (e.g., on a plane, see Figure 11) by correctly answering a set of previously enrolled questions. This can be done without any help desk interaction and offers more convenient recovery than via challenge/response. In SafeGuard Enterprise version 5.40, Local Selfhelp is offered for standalone mode only;

version 5.50 offers Local Selfhelp in all modes, thus replacing the previous Web Selfhelp module.

Finally, SafeGuard Enterprise also provides an API that allows customers to build or integrate SafeGuard recovery functions into their own custom help desk application.

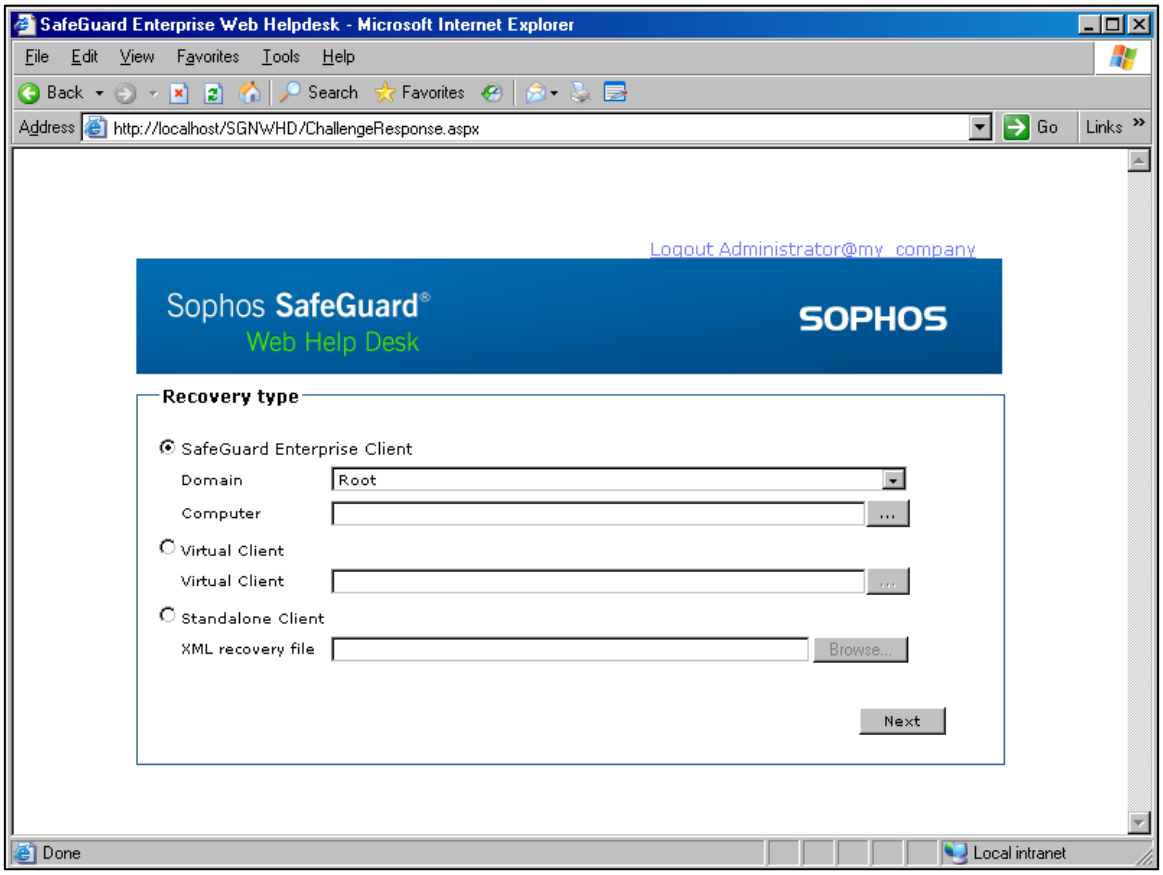


Figure 9: SafeGuard Web Helpdesk

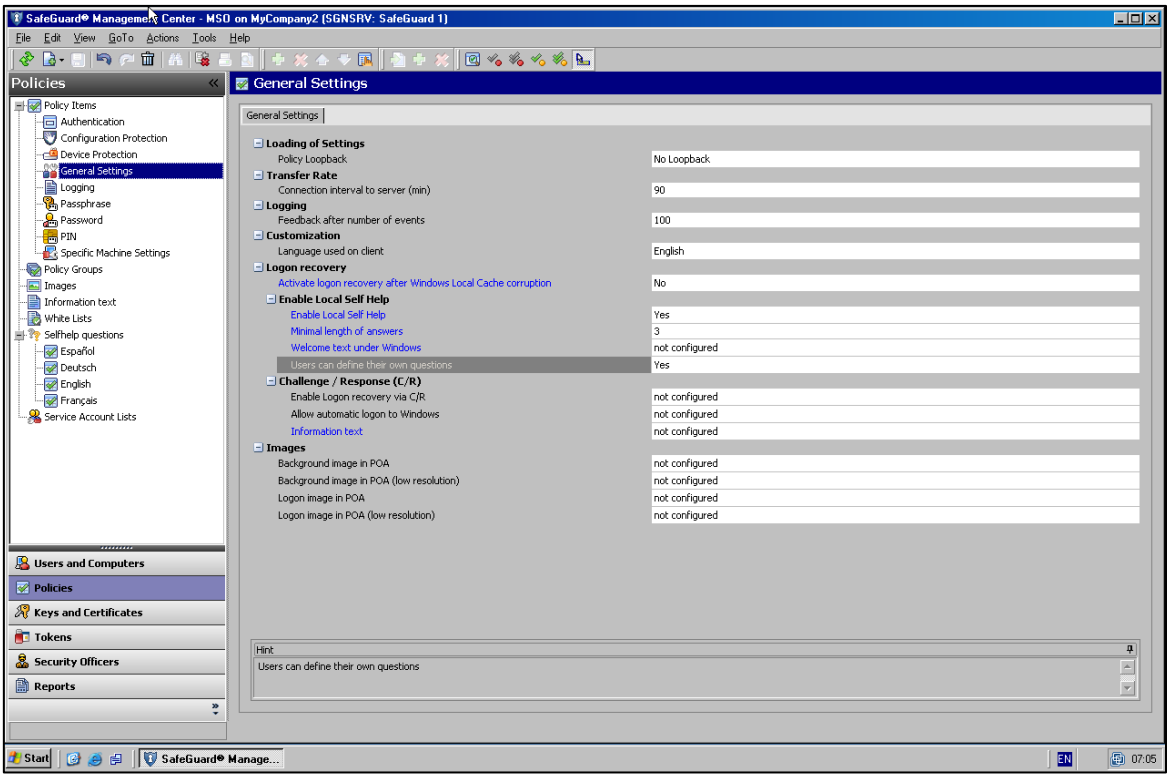


Figure 10: SafeGuard Local Selfhelp management

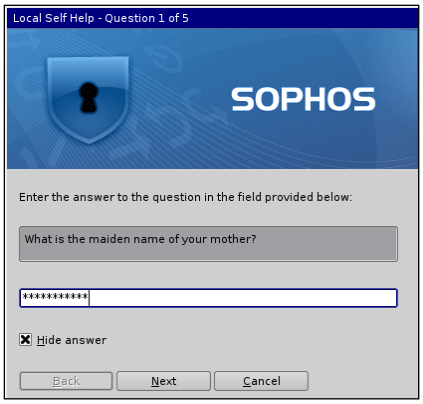

Local Self Help - Question 1 of 5
SOPHOS
Enter the answer to the question in the field provided below:
What is the maiden name of your mother?
Hide answer
Back
Next
Cancel

Figure 11: SafeGuard Local Selfhelp in POA

5 SafeGuard Enterprise encryption methods

5.1 Overview

The primary purposes of the Device Encryption and Data Exchange modules are to protect data saved on a client or removable storage medium, and to authenticate the authorized user at a very early point in time (Power On Authentication for Device Encryption).

5.2 Smart Media Encryption

To encrypt media, SafeGuard Enterprise uses sector-based encryption functionality, which is also provided in SafeGuard Easy, and file-based encryption, which is transparent to the user. By combining these two technologies in one product (Smart Media Encryption), SafeGuard Enterprise is very flexible in the ways it can be implemented to meet customer requirements.

The characteristics of the **sector-based** encryption method are:

- The entire data medium is encrypted sector by sector, including all temporary files or swapfiles and the directory information.
- On a PC on which SafeGuard is not installed, data media that have undergone sector-based encryption are shown as unformatted data media because the operating system cannot read the directory information at all.
- This method is also suitable for the boot volume from which the operating system boots.
- This method is not suitable for optical media such as CDs/DVDs.
- Plaintext and encrypted data cannot be mixed on the same data medium (all data is encrypted).
- The encryption is completely transparent to users.

The characteristics of the **file-based** encryption method are:

- The entire data medium is encrypted at the file level; directory information remains in plaintext.
- On a PC on which SafeGuard is installed, data media that have undergone file-based encryption are shown as normal data media because the operating system can read the directory information on them. Plaintext data can be exchanged with systems of this kind.

- This method is not suitable for the boot volume from which the operating system boots.
- However, it is suitable for optical media such as CDs/DVDs.
- One data medium can contain a mixture of plaintext and encrypted data.
- The encryption is completely transparent to users.

In SafeGuard Enterprise, it is now possible for the first time to unite the benefits of both worlds in one product. Specializing in data medium encryption keeps the policy settings simple and easy to understand because there is no need for complex rules for individual files or directories.

Overview of supported device encryption methods and properties:

	Sector-based SGN device encryption	**File-based SGN device encryption**	**Vista/7 BitLocker[3]**
Supported OS	Windows XP, 2003, Vista/7 32[2]/64[4]	Windows XP, 2003, Vista/7 32[2]/64[3]	Windows 2008(R2)/Vista/7 32/64 Enterprise and Ultimate editions
Usable to encrypt boot partition	☑	☒	☑
Smartcard, multi-user, challenge/response support for pre-boot authentication	☑	☒	☒
Usable to encrypt secondary partitions	☑	☑	☑[5]
Usable to encrypt non-optical removable media	☑	☑	☑[6]
Usable to encrypt optical media (CD/DVD)	☒	☑	☒

[3] BitLocker management and Windows Vista support are available since SafeGuard Enterprise version 5.20.

[4] Windows Vista and Windows 7 64-bit were first supported in SafeGuard Enterprise 5.50.

[5] Requires SGN management or Vista SP1

[6] Windows 7 only

Allows optional mix of plaintext and encrypted text	☒	☑	☒
Media directory information is accessible on non-SafeGuard clients	☒	☑	☒
Encrypted data can be read on third-party machines (portable reader)	☒	☑	☑[7]
Encrypted data can be written/updated on third-party machines (portable reader/writer)	☒	☑	☒
Included in SGN BitLocker client package	☒	☑	☑
Included in SGN Device Encryption client	☑	☑	☑

Note that the future SafeGuard Enterprise FileShare module will, as the successor of SafeGuard LAN Crypt, also offer file-based encryption with complex rules based on file or folder types and names, both locally and on network shares. In contrast, the current file-based device encryption uses the same filter technology with simpler policies on the device level only.

Optical media such as CDs and DVDs[8] may be encrypted easily by integrating SafeGuard Data Exchange into Windows Explorer, which informs users about the encryption policy and allows them to adjust settings within their policy rights before the files are actually burned (see Figure 12).

[7] Requires Windows 7 BitLocker To Go; usage requires FAT formatted media and files to be copied on the local desktop first. It is not possible to write to encrypted media under Windows Vista or XP. In contrast, SafeGuard Enterprise offers transparent media read/write use (FAT and NTFS) on all supported Windows platforms. The SGN Portable tool allows read/write access on encrypted files directly on the media on external/unmanaged PCs that do not have SafeGuard Enterprise installed.

[8] Hint: Windows XP allows CD burning only via the built-in functionality. To burn encrypted DVDs under Windows XP, the additional use of third-party packet writing software such as Nero InCD is required: http://www.nero.com/eng/downloads-nero9-tools-utilities.html.

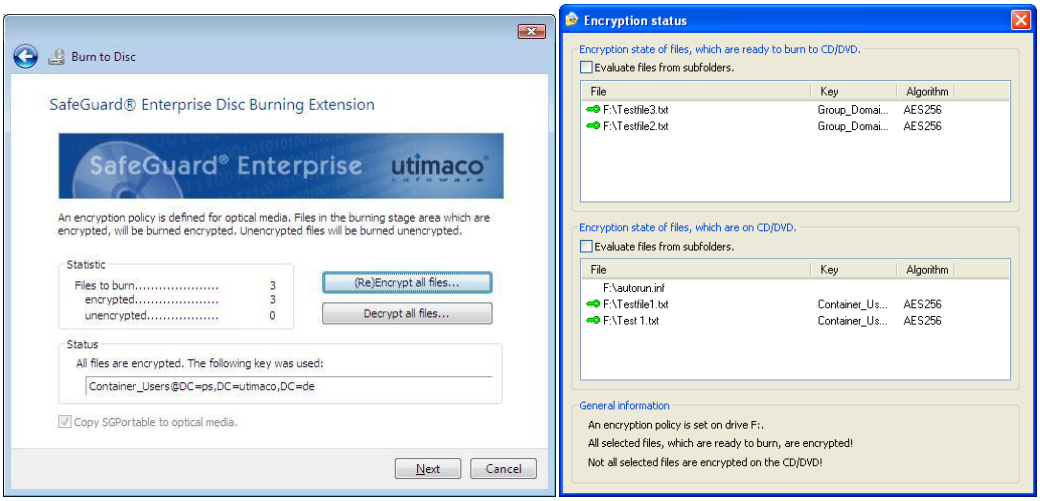

Burn to Disc
SafeGuard® Enterprise Disc Burning Extension
SafeGuard® Enterprise utimaco
An encryption policy is defined for optical media. Files in the burning stage area which are encrypted, will be burned encrypted. Unencrypted files will be burned unencrypted.
Statistic
Files to burn..... 3
encrypted..... 3
unencrypted..... 0
(Re)Encrypt all files...
Decrypt all files...
Status
All files are encrypted. The following key was used:
Container_Users@DC=ps,DC=utimaco,DC=de
Copy SGPortable to optical media.
Next
Cancel
Encryption status
Encryption state of files, which are ready to burn to CD/DVD.
Evaluate files from subfolders.
File
Key
Algorithm
F:\Testfile3.txt Group_Domai... AES256
F:\Testfile2.txt Group_Domai... AES256
Encryption state of files, which are on CD/DVD.
Evaluate files from subfolders.
File
Key
Algorithm
F:\autorun.inf
F:\Testfile1.txt Container_Us... AES256
F:\Test 1.txt Container_Us... AES256
General information
An encryption policy is set on drive F:.
All selected files, which are ready to burn, are encrypted!
Not all selected files are encrypted on the CD/DVD!

Figure 12: Integration in Windows Vista and XP Explorer for burning encrypted optical media

5.3 Power On Authentication

SafeGuard Enterprise identifies the user before the operating system even boots. To do so, a dedicated SafeGuard Enterprise kernel, which is hidden on the hard disk to protect it against tampering, runs before the operating system. Users must authenticate themselves correctly to this SafeGuard Enterprise function before the actual operating system of the encrypted partition (Windows) boots, and then they are automatically logged on to Windows. A similar approach applies if the client is switched on when it is in hibernation (Suspend to Disk) mode.

Compared to SafeGuard Easy, BitLocker and comparable products, SafeGuard Enterprise's Power On Authentication offers these benefits, among others:

- A graphical user interface with mouse support and moveable windows, making it easy to use (see Figure 13)
- A policy for corporate customers to tailor the GUI layout (e.g., background picture, logon bitmap, welcome message)
- Support for a multitude of card readers and smartcards
- Biometric fingerprint logon (see Figure 14): support for pre-boot and Windows logons; password/UID optional; single sign-on is also supported; currently available only for Lenovo laptops/desktops with UPEK or Authentec fingerprint readers. The list of supported readers is available via Knowledge Base article on sophos.com.

- Support for Windows user accounts and passwords right at the pre-boot stage, so there is no need for users to remember separate access data
- Support for Unicode, which enables support for passwords or user interfaces in different languages

Figure 13: Graphical POA

Figure 14: POA by fingerprint

5.4 Smartcard and token integration

Optionally, SafeGuard Enterprise supports the use of smartcards and X.509 certificates from external PKIs for user login and for securing the keyring. It supports smartcards both at the operating system level (e.g., for logon to the Management Console in Windows) and in POA. If required, SafeGuard Enterprise also offers the option to use smartcards without certificates for logon by using a protected, saved, single sign-on table instead of the RSA key.

POA's special architecture supports a very wide range of hardware, and this will be continually extended. For details, see Section 6.1.

Sophos has also issued a separate white paper for smartcard and token integration, [SGN Smartcard].

5.5 Emergency scenarios

For SafeGuard Enterprise users, forgotten passwords and lost tokens are no problem. With the help of the challenge/response procedure or Selfhelp option, which are already proven through use in other SafeGuard products, users can regain access to their data quickly and securely, even if they are on the move.

Alternatively, thanks to the new SafeGuard Enterprise keyring concept, a data medium can also be used in another computer or by another user with a suitable key in his or her keyring.

Even if the operating system itself is no longer able to boot, emergency tools are provided that run under Windows PE, and that the administrator can use to boot the computer from any bootable external media and repair the encrypted hard disk. Recovery media can even be personalized and if necessary revoked (e.g., if their "owner" leaves the company). These recovery media are called Virtual Clients.

5.6 SafeGuard Enterprise BitLocker client

SafeGuard Enterprise enables all the BitLocker functions provided in a Windows Vista and Windows 7 Enterprise or Ultimate installation to be managed from the SafeGuard Enterprise Management Center (see Figure 15). This means that the BitLocker policies are assigned from the SGN Management Center, transported to the client via the SGN mechanism and executed there. The encryption status of the BitLocker clients is also displayed in SGN's central event log and status overview. When the administrator is involved in managing BitLocker,

SafeGuard Enterprise takes over many tasks that the administrator would otherwise have to perform manually, using scripts (e.g., scripts for validation of the client encryption state, or for encrypting non-boot volumes, as well as settings in different group policy objects (GPO) for memory stick and validation profiles). SGN also performs backup and recovery for BitLocker keys.

BitLocker can only encrypt local hard disks, so the SGN BitLocker client provides functions for file-based removable media encryption that are compatible with SafeGuard Data Exchange. Optionally, SGN also enables BitLocker to encrypt additional partitions besides the boot partition (this functionality requires Vista SP1). A mixed-mode environment with both BitLocker and sector-based SGN Device Encryption is not possible on the same client.

Customers who do not have a 100% Vista Enterprise or Ultimate environment, or who still want to implement additional security components such as removable media encryption, will especially value the joint administration from one console in SafeGuard Enterprise.

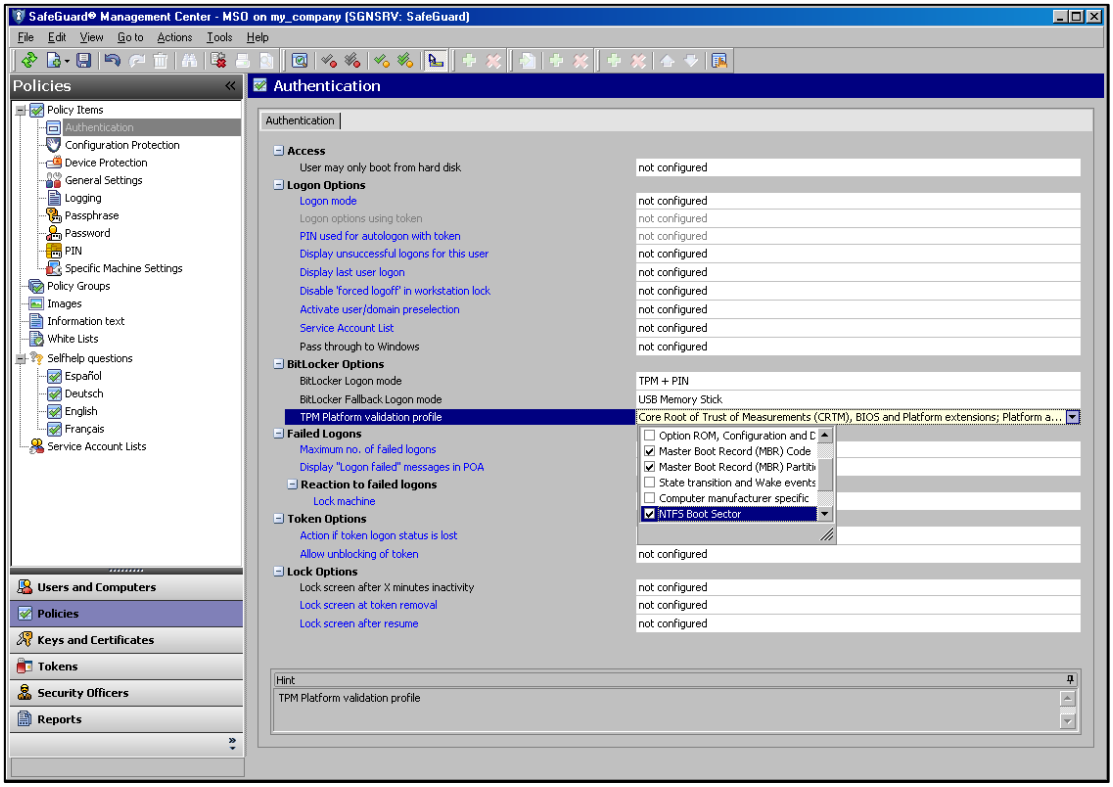


Figure 15: BitLocker settings in SGN Management Center

Before rolling out a hard disk encryption solution, companies should carefully weigh whether to use the BitLocker or the SafeGuard Enterprise method. The SafeGuard Enterprise Device Encryption method offers some benefits over BitLocker, such as:

- It supports Windows XP and **all** Vista/Windows 7 variants—other OSs will follow in the future.
  (BitLocker only supports Vista Enterprise and Ultimate editions.)
- It requires no special hard disk partition for installation.
  (BitLocker requires its own partition.)
- It supports different smartcards and tokens for pre-boot authentication.
  (BitLocker supports no smartcards—only memory sticks that contain a copyable key file.)
- It supports and differentiates between different users during pre-boot authentication.
  (BitLocker does not differentiate between different users.)
- It provides a way for forgotten passwords to be reset via the secure, dynamic challenge/response procedure.
  (BitLocker uses a fixed 48-digit recovery key.)
- It has a graphical user interface in pre-boot authentication.
  (BitLocker has only text.)
- It accepts complex passwords and password rules that are synchronized with Windows.
  (BitLocker only permits a TPM PIN.)
- It also allows sector-based encryption for removable media across older Windows platforms such as Windows XP and Vista.
  (BitLocker encrypts removable media only under Windows 7! Together with the SGN BitLocker client, file-based removable media encryption via SafeGuard Enterprise is possible.)

See the Sophos white paper [SGN BitLocker] for more information about the advantages of and differences between both solutions.

6 Appendix

6.1 Technical data

Supported operating systems for SGN client:
Windows 7 32/64 bit
Windows Vista 32/64 bit SP1/SP2
Windows XP 32 bit SP2/SP3

Supported operating systems:
SafeGuard Enterprise Server, 32 and 64 bit:
Windows Server 2003 R2 including IIS and Active Directory
Windows Server 2008 (R2) including IIS and Active Directory

Management Center:
Windows 7 32/64 bit
Windows Vista 32/64 bit SP1/SP2
Windows XP 32 bit SP2/SP3

Languages of SafeGuard Enterprise user interface:
Full product: English, German, French, Japanese
Client only: Spanish, Italian

Supported standards:
Encryption: AES 256 bit, RSA
Hash: SHA-1, SHA-256, SHA-384, SHA-512
Various: PKCS #1, PKCS #5, PKCS #7, PKCS #11, PKCS #12, PKCS #15, X.509 certificates, LDAP, Microsoft Cryptographic Service Provider (CSP), SOAP, XML, SSL, TCG, CCID, Kerberos
Certifications: FIPS 140-2 certified, Common Criteria EAL 3+ certified, CC EAL 4 in work, Aladdin and EnCase enabled

Database for the SafeGuard Enterprise Server:
Microsoft SQL Server 2005 or 2008 (not supplied)
Microsoft SQL Server Express edition (available free of charge from Microsoft)

Supported models for fingerprint authentication:
Most Lenovo models with UPEK or Authentec sensors are supported except UPEK without a companion chip. A list of supported models can be found here.

Supported card readers and smartcards:

Please refer to the 'SafeGuard Enterprise Smartcard integration' whitepaper for a complete compatibility list of smartcards, smartcard readers, USB token and compatible middleware.

6.2 Migration from existing SafeGuard products

Utimaco's existing product portfolio will continue to be developed and maintained, in parallel, in smaller releases, but in the medium term those products will be absorbed into SafeGuard Enterprise. Note that in version 5.30 onward, it is possible to do an in-place migration from SafeGuard Easy 4.x or Sophos SafeGuard Disk Encryption to SafeGuard Enterprise without needing to uninstall the product or re-encrypt the hard disk or encrypted removable media beforehand. For details, see the white paper "Migration overview: SafeGuard → SafeGuard Enterprise".

6.3 New in SafeGuard Enterprise 6

This white paper has been adapted to SafeGuard Enterprise 6 but does not describe all new functions in extensive detail. For a comprehensive list of what's new, please see the Sophos white paper 'SafeGuard Enterprise 6 What's New', or the user manual.

7 Abbreviations

AES	Advanced Encryption Standard; an international standardized modern encryption algorithm with 128- or 256-bit key lengths. It is based on the Rijndael algorithm and the current international standard for bulk data encryption.
CSP	Cryptographic Service Provider; Microsoft interface for integrating cryptography in Windows applications.
ESDP	Endpoint Security and Data protection; Sophos's complete suite for malware- and data protection. Provides full disk encryption for local harddrives via a bundle of a simplified variant of SafeGuard Enterprise Device Encryption for Windows or MacOS.
ESS	Embedded Security Subsystem; a cryptographic chip and driver software in Lenovo PC systems that complies with the specifications of the Trusted Computing Group (TCG—see below).
GINA	Graphical Identification and Authentication; an interface defined by Microsoft that controls the desktop and login to Windows NT/2000/XP. In Windows Vista and Windows 7 the GINA was replaced by Credential Providers.
IDEA	International Data Encryption Algorithm; a symmetrical encryption algorithm developed in 1990. It uses a key length of 128 bits.
PDA	Personal digital assistant; a synonym for computers that are smaller than a notebook. They usually run with specially tailored, cut-down variants of familiar operating systems.
PIM	Personal information management; a collective term that describes typical applications that are used every day (e.g., Calendar, Contacts, To-do lists, Notes), which are frequently already installed in PDAs.
PIN	Personal identification number; a kind of password that identifies the user. This term is normally used in connection with smartcards.

PKCS #11	A non-platform-specific standard used to integrate cryptographic hardware such as smartcards in security applications.
POA	Power On Authentication; user authentication directly after the device is switched on, but before the operating system boots.
RSOP	Resultant Set of Policy; a simulation procedure for determining a policy that has resulted from hierarchical inheritance. It is offered as a function in the SafeGuard Enterprise Management Console.
SGE	SafeGuard Easy; the predecessor of SafeGuard Device Encryption.
SGN	SafeGuard Enterprise; Sophos's flagship product for disk and removable media encryption, port control and key management for Windows.
SSO	Single sign-on; a synonym for the creation of a user environment in which users only require one password to start the system. After this, the system automatically presents other passwords.
TCG	Trusted Computing Group; an international association of hardware and software manufacturers that drafts specifications for hardware-based PC security.
TPM	Trusted Platform Module; a cryptographic hardware chip that complies with the TCG specifications.
UID	User ID; a username that the user enters during logon to the security system.
UVM	User Verification Manager; Lenovo authentication components for its PCs at Windows (GINA) level.
VPN	Virtual private network; a method used to encrypt network traffic at the IP packet level and so guarantee the confidentiality of data that is transferred over public networks (i.e., over the internet) to participants who also have the correct key data.

8 Literature and Sources

[Mobile security] Security for mobile PCs and data media

Sophos white paper

[SGN BitLocker] Windows 7 BitLocker and its Relation to SafeGuard Enterprise

Sophos technical white paper

[SGN Migration] Migration overview: SafeGuard → SafeGuard Enterprise

Sophos white paper

[SGN SCOM] SafeGuard Enterprise Management Pack for Microsoft Systems Center Operations Manager 2007

Sophos white paper

[SGN Smartcard] SafeGuard Enterprise Smartcard integration

Sophos white paper

Boston, USA | Oxford, UK
© Copyright 2012, Sophos Ltd

All registered trademarks and copyrights are understood and recognized by Sophos.
No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means without the prior written permission of the publishers.

SOPHOS
WWW.SOPHOS.COM